14.02.2007 - Tobias Vößing

Protokoll - Anwendungsfach Mathematik - Hauptstudium

Graphentheorie 1 und 2, Kryptographie 1 und 2

Die Prüfung ging über ca. 35-40 Minuten, davon etwa 20 Minuten Graphentheorie. Die Prüfer waren Prof. Volkmann für Graphentheorie und Prof. Mathar für Kryptographie. Ich gebe den Ablauf aus dem Gedächtnis mit dadurch verbundenen Ungenauigkeiten wieder. Bei Fragen: `Tobias.Voessing@rwth-aachen.de`.
Der kleine Fisch bin ich ($\propto$), der Punkt ($\odot$) ist der jew. Prof.

Graphentheorie

$\odot$ Jemand gibt Ihnen eine große Adjazenzmatrix. Wie prüfen Sie, ob es einen Kreis gibt?

$\propto$ Ich würde $\mu(G)$ bestimmen. $n(G)$ und $m(G)$ ergeben sich sofort aus der Matrix. $\kappa(G)$ kann man mit Hilfe eines Algorithmus bestimmen, der die Zusammenhangskomponenten bestimmt. Falls $\mu(G) \geq 1$ gibt es einen Kreis, denn $\mu(G) = 0 \iff G$ Wald.

$\odot$ Können Sie den Algorithmus kurz beschreiben?

$\propto$ Man wählt eine beliebige Ecke x und betrachtet die Nachbarn $N(x)$. Dann schaut man auf die Nachbarn der Nachbarn und erhält ggf. neue Ecken usw. Wenn man am Ende alle Ecken $E(G)$ einmal angetroffen hat, ist der Graph zusammenhängend. Sonst führt man dieselben Schritte mit einer noch nicht betrachteten Ecke weiter.

$\odot$ Wann hat der Graph denn genau einen Kreis?

$\propto$ Ich verstand, wann der Graph genau ein Kreis ist und antortete, dass alle Ecken den Grad 2 haben müssten. Prof. Volkmann wies mich darauf hin und ich brachte $\mu(G) = 1 \iff \nu(G) = 1$.

$\odot$ Wie sieht es mit $\mu(G) \geq 2$ aus? Kann man da auch so eine Aussage treffen?

$\propto$ Nein, die Äquivalenz zwischen μ und ν gilt nur für 0 und 1. Ich malte dann einen Graphen mit $\mu(G) = 2$ und $\nu(G) = 3$ auf (ein Dreikreis und ein Vierkreis mit einer gemeinsamen Kante).

$\odot$ Thema Gradsequenzen: Wann ist eine gegebene Gradsequenz eine von einem Baum?

$\propto$ Genau dann, wenn $\sum_{i=1}^{n} d_i = 2n - 2$. Ich wies auf $n \geq 2$ hin und erläuterte den Beweis analog zu dem aus dem Skript: Induktion nach n.

$\odot$ Ich behaupte mal, dass jeder Graph G so orientierbar sei, dass für jede Ecke x gilt: $|d^+(x) - d^-(x)| \leq 1$. Was sagen Sie dazu?

$\propto$ Ich kannte diese Frage zu meinem Glück aus einer Prüfung eines Gleichgesinnten und habe mir den Beweis schon in der Vorbereitung zurecht legen können: Nach HSL hat jeder Graph gerade viele Ecken ungeraden Grades. Seien diese Ecken $x_1, \ldots, x_{2p}$. Wir fassen sie zu Paaren (x_i, x_{i+1}) zusammen und verbinden diese mit jeweils einer Kante. Dieser Graph ist eulersch und hat eine Orientierung mit $|d^+(x) - d^-(x)| = 0$. Entfert man die hinzugenommenen Kanten wieder, stolpert man über die gesuchte Orientierung.

$\odot$ Kommen wir mal zu multipartiten Turnieren. Hat jedes stark zusammenhängende multipartite Turnier einen Hamiltonkreis?

$\propto$ Nein. Bekanntes Gegenbeispiel: Ein p-partites Turnier mit den Partitionsmengen $E_1 \to E_2 \to \ldots \to E_p \to E_1$ mit $|E_1| = 1$ und $|E_i| \geq 2$ für $i = 2, \ldots, p$ ($E_i \to E_j$ meint E_i dominiert E_j).

$\odot$ Können sie beweisen, dass jedes stark zusammenhängende p-partite Turnier einen Kreis der Länge p hat?

$\propto$ Ich überlegte und erwähnte eher ausweichend, dass jede Ecke wohl auf einem längsten Kreis läge. Kam aber nach einem kläglichen Versuch, einen Ansatz zu finden, zu dem Entschluss, hier passen zu müssen.

$\odot$ Nennen Sie mir alle Graphen, für die $\gamma(G) = \alpha(G)$ gilt.

$\propto$ Ich nannte C_4 und $H \circ K_1$. Prof. Volkmann wollte leider den Beweis, dass dies alle seien. Ich überlegte etwas und wurde mit dem Hinweis unterbrochen, dass dieser nicht so trivial sei um ihn sich noch schnell aus dem Ärmel zu schütteln. Schade.

$\odot$ Sind bipartite Graphen perfekt? Was ist das Kriterium für perfekt?

$\propto$ Ein Graph G ist perfekt wenn $\alpha(G') = \theta(G')$ für alle induzierten Teilgraphen G' erfüllt wird. Die induzierten Teilgraphen eines bipartiten Graphen sind auch bipartit. Es reicht hier also aus, $\alpha(G) = \theta(G)$ zu zeigen, was ich dann auch genau wie im Skript tat.

Kryptographie

$\odot$ Ich habe mir ein Kryptosystem ausgedacht: $(m_1 \ldots m_n)$ sei der Klartext über dem uns bekannten Alphabet, $(k_1, \ldots, k_s)$ das Schlüsselwort und die Verschlüsselung laufe blockweise $c_i = m_i + k_{i \bmod s} \mod 26$. Ist dieses Kryptosystem perfekt sicher?

$\propto$ Das erinnert mich stark an Vignere. Man sieht, dass die Spalten $c_i, c_{i+s}, c_{i+2s}, \ldots$ monoalphabetisch verschlüsselt werden. Man erhält mit Häufigkeitsanalyse Rückschlüsse auf den Klartext. Das System kann also nicht perfekt sicher sein.

$\odot$ Wie würden Sie vorgehen, ein solches System zu knacken?

$\propto$ Zuerst benötigt man die Länge s des Schlüsselwortes. Ich erläuterte hier das Verfahren von Kasiski-Babbage, das man anwenden kann, wenn man Abschnitte im Kryptotext findet, die gleich sind.

$\odot$ Wir hatten aber auch einen Test, der mit statistischen Mitteln arbeitet.

∝ Ich vermutete richtig, dass der Friedmann-Test gemeint war und versuchte mich an einer Erklärung. Prof. Mathar brachte ein wenig Struktur in meine etwas sprunghaften Argumente indem er mich nacheinander die Zufallsvariable I_C und dann deren Erwartungstreue nachweisen lies. Ich wollte gerade ansetzen, die Idee des Friedmann-Tests in einer Formel auszudrücken, als ich unterbrochen wurde mit dem Hinweis, dass mein Vorgehen etwas *unstochastisch* sei. Er könne aber absehen, dass ich den Test rekonstruieren kann.

⊙ Kommen wir zu den asymmetrischen Verfahren. Es gibt hier zwei bedeutende schwierige Probleme: Diskreter Logarithmus und Faktorisierung. Was ist überhaupt ein diskreter Logarithmus modulo Primzahl?

∝ Man benötigt eine Primitivwurzel $a \in Z_p^*$. a ist dann Erzeuger von Z_p^*, also $\text{ord}(a) = \varphi(p) = p - 1$. Zu jedem $y \in Z_p^*$ existiert ein $x \in Z_p^*$, so dass $y = a^x \mod p$. x ist diskreter Logarithmus von y zur Basis a.

⊙ Da braucht man für ausreichend Sicherheit eine recht große Primzahl. Wie bekommt man die?

∝ Es gibt probabilistische Algorithmen, die mit hoher Sicherheit eine Zahl als Primzahl identifizieren. Man wählt eine große Zufallszahl und prüft, ob diese zusammengesetzt ist.

⊙ Welche Algorithmen kennen sie?

∝ Z.B. Miller-Rabin. Sei n die Zahl, die man prüfen möchte. Stelle n als $q \cdot 2^k + 1$ mit maximalem k dar. Wählt man zufällig ein $a \in Z_n^*$, ist a ein Zeuge für n zusammengesetzt, falls $a^q \not\equiv \pm 1$ und $a^{q \cdot 2^i} \not\equiv -1$ für alle $i = 1, \ldots, k - 1$.

⊙ Manchmal ist das Resultat dieses Tests aber auch bedenklich. Wieso?

∝ Es gibt starke Pseudoprimzahlen, für die es wenig oder keine Zeugen gibt. Allgemein sind aber ca. $\frac{3}{4}$ aller Elemente aus Z_n^* Zeugen.

⊙ Ok und durch mehrfaches Anwenden verbessert man dann die Sicherheit des Algorithmus. Kommen wir zurück zum diskreten Logarithmus. Wir haben die Primzahl p, wie kommt man an eine Primitivwurzel?

∝ Das ist für beliebige p bestimmt nicht so einfach. Es gibt einen Satz, den man ausnutzen kann: Sind $p_1, \ldots, p_k$ alle Primteiler von $p - 1$, so ist a Primitivwurzel gdw. $a^{\frac{p-1}{p_i}} \not\equiv 1$ für alle $i = 1, \ldots, k$. Sucht man sich zwei Primzahlen p und q, so dass $p = 2q + 1$, dann muss man nur $a^2 \not\equiv 1$ und $a^q \not\equiv 1$ prüfen.

⊙ Sie haben da bestimmt den *Intruder In The Middle*-Angriff vor Augen, der ausnutzt, dass a^q die Ordnung 2 hat. Wieso geht man nicht einfach hin und nimmt zwei Primzahlen p und q, so dass z.B. $p = 7q + 1$ um das Problem abzuschwächen?

∝ Prof. Mathar murmelte, diese Frage sei wirklich blöd gewesen. Prof. Volkmann musste ebenfalls grinsen. Ich verstand den Witz noch nicht ganz und stand ein bisschen auf dem Schlauch. Ich schmiss etwas ungewiss in die amüsierte Runde, man müsse erstmal nachweisen, dass es solche Primzahlen überhaupt gäbe. Dann fiel es mir wie Schuppen aus den Haaren: $7q$ ist ungerade, d.h. $7q+1$ ist gerade, ergo gibt es keine solche Primzahl.

$\odot$ Ein kryptographisches Verfahren, dass den diskreten Logarithmus benutzt ist ElGamal. Können Sie das erläutern?

$\propto$ Ich erklärte private- und public-key und zeigte die Verschlüsselung.

$\odot$ Warum sollte man denn den session-key zufällig wählen? Kann ich den nicht festsetzen auf z.B. 3?

$\propto$ Nein, denn dann kann man mit etwas Glück (bestimmte Terme müssen invertierbar sein) aus zwei verschiedenen verschlüsselten Nachrichten den private-key ausrechnen.

$\odot$ Welchen Angriff aus ElGamal kennen Sie?

$\propto$ Z.B. Diffie-Hellmann-Problem lösen. Ich konnte nicht mehr ausholen, denn die Zeit war um.

Fazit: Ich habe mich für Graphentheorie auf die Kapitel 1-4 mit großer Sorgfalt vorbereitet, was sich gelohnt hat. Vor allem Fragen über Kreise, Wälder, Kaktusgraphen, Gradsequenzen und Digraphen sind bei Prof. Volkmann sehr beliebt. Für die weiteren Kapitel lernte ich hauptsächlich die Standardsätze (z.B. Moon, Petersen, Katerinis, König, Tutte, König-Hall, ...) und beliebte Skizzen um Gegenbeispiele bringen zu können. Rückblickend stelle ich fest, dass man auch die anderen Kapitel mit etwas mehr Tiefgang lernen sollte. Die Graphenparameter α, α_0, β und γ sind in fast jeder Prüfung vertreten. Für viele Sätze sollte man auch den Beweis parat haben.
In Kryptographie sind nicht nur die Verfahren sondern ebenfalls die Analysen dieser wichtig (Korrektheit, Schwachstellen und Angriffspunkte, praktische Durchführung). Eines der drei bekannten asymmetrischen Verfahren (RSA, Rabin, ElGamal) kommt mit Sicherheit in jeder Prüfung vor.